IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Messaoud Benantar		
Assignee:	International Business Machines Corporation		
Title:	Method and System for Network Single Sign-on Using a Public Key Certificate and an Associated Attribute Certificate		
Serial No.:	09/821,064	Filing Date:	March 29, 2001
Examiner:	Christopher J. Brown	Group Art Unit:	2134
Docket No.:	AUS920010140US1	Customer No.	65362

Austin, Texas
December 7, 2007

FILED ELECTRONICALLY

APPEAL BRIEF UNDER 37 CFR § 41.37

Dear Sir:

Applicant submits this Appeal Brief pursuant to the Notice of Panel Decision from Pre-Appeal Brief Review mailed in this case on November 8, 2007. The fee for this Appeal Brief is being paid electronically via the USPTO EFS. The Board is authorized to deduct any other amounts required for this appeal brief and to credit any amounts overpaid to Deposit Account. No. 09-0447.

I. REAL PARTY IN INTEREST - 37 CFR § 41.37(c)(1)(i)

The real party in interest is the assignee, International Business Machines Corporation, as named in the caption above and as evidenced by the assignment set forth at Reel 011687, Frame 0358.

II. RELATED APPEALS AND INTERFERENCES - 37 CFR § 41.37(c)(1)(ii)

Based on information and belief, there are no appeals or interferences that could directly affect or be directly affected by or have a bearing on the decision by the board of patent appeals and interferences in the pending appeal. Pursuant to current Patent Office practice, Appendix "A" contains copies of all decisions rendered by a court or the Board in this "Related Appeals and Interferences" section, and is intentionally provided as an empty appendix.

III. STATUS OF CLAIMS - 37 CFR § 41.37(c)(1)(iii)

Claims 1-26 are pending in the application. Claims 1-26 stand rejected. The rejection of claims 1-26 is appealed. Appendix "B" contains the full set of pending claims.

IV. STATUS OF AMENDMENTS - 37 CFR § 41.37(c)(1)(iv)

In an Amendment and Response to Final Office Action dated September 4, 2007, Applicant proposed to amend claims 3, 13 and 21, but these amendments were not entered. *See*, Advisory Action, (September 13, 2007). For the reasons set forth hereinbelow, Applicant respectfully traverses the pending art rejections, and further notes that claim 9 has not been rejected over the cited references, and therefore requests that a notice of allowability be issued for at least claim 9 and claim 10 (which depends from claim 9).

V. SUMMARY OF CLAIMED SUBJECT MATTER - 37 CFR § 41.37(c)(1)(v)

The subject matter defined in independent claim 1 may be understood with reference to the example embodiments depicted in Figures 5 and 7 which depict a method for a network single sign-on (SSO) authentication process using attribute certificates. A user requesting access to protected resources, such as legacy applications, must have the user's authentication data verified prior to being provided access. When the user's authentication data is encrypted into an attribute certificate, a user's request to access the protected resource is processed by a single sign-on (SSO) agent that performs an initial authentication process against the user. Thus, the method begins at step 702 when the SSO agent (e.g., 510) receives an initial authentication request for a user (e.g., 500) and then authenticates the user 500 as requested. *See*, *e.g.*, Application, ¶ 75 ("After an initial configuration phase, which is discussed in more detail below, client network single sign-on (SSO) manager application 510 performs password management for user 500 such that, after user 500 completes a single authentication process with client SSO manager

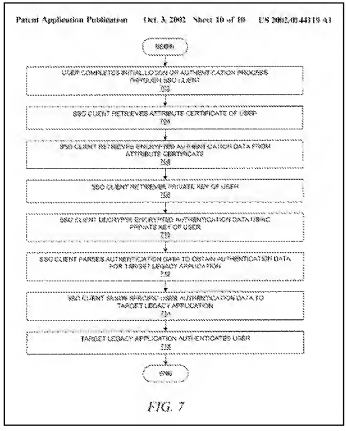

FIG. 7

510, client SSO manager 510 acts as an authentication agent to perform subsequent authentication processes that are required by target legacy applications 502."). In addition to authenticating the user, the SSO also authenticates the user for subsequent authentication requests made by the SSO agent by using authentication data contained within the attribute certificate. In Figure 7, this occurs at step 704, where the SSO agent 510 retrieves an attribute certificate 530 associated with the user 500, and at steps 706-716, where the SSO agent 510 uses the authentication data within the attribute certificate 530 to authenticate the user 500 for subsequent authentication requests. Application, ¶ 75 ("[C]lient SSO manager 510 acts as an authentication agent to perform subsequent authentication processes that are required by target legacy applications 502."). In particular, the SSO agent 510 forwards the required authentication data to the protected resource, and the protected resource then authenticates a user based on the provided authentication data. *See*, *e.g.*, Application, ¶ 96 ("The required authentication data is then forwarded to application server 504 as appropriate, and user 500 is then able to use the legacy application. If the user decides to access another protected resource, then the user is not burdened with another authentication challenge.")

To comply with 37 CFR § 41.37(c)(1)(v), a color-coded comparison of independent claim 1 (including reference characters from Figure 5) and the relevant portion of Figure 7 is set forth below:

1. A method for an authentication process within a data processing system, the method comprising:

receiving at a single sign-on (SSO) agent (510) an initial authentication request for a user (500);

authenticating the user at the SSO agent (510) for the initial authentication request;

retrieving by the SSO agent an attribute certificate (530) associated with the user (500); and

authenticating the user (500) for subsequent authentication requests via the SSO agent (510) using authentication data (526) within the attribute certificate (530).

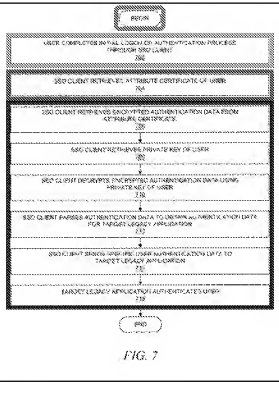

FIG. 7

In further compliance with 37 CFR § 41.37(c)(1)(v), a color-coded comparison of selected Figures from the application and each of the pending independent claims is attached at Appendix "C" to provide a concise explanation of the subject matter defined in each independent claim. The subject matter of the independent claims is set forth in the specification at U.S. Patent Pub. No. 20020144119, ¶¶ 12, 72-97 and 104-113, though additional contextual description is provided in the application.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

In the Final Office Action the Examiner rejected claims 1-26 under 35 U.S.C. § 103(a) as being unpatentable over various combinations of U.S. Patent No. 6,691,232 to Wood ("Wood"), U.S. Patent No. 5,339,403 to Parker ("Parker"), U.S. Patent No. 6,766,454 to Riggins ("Riggins"), U.S. Patent No. 5,339,403 to Olden ("Olden"), and U.S. Patent No. 6,754,829 to Butt ("Butt"). Applicant filed an Amendment after Final proposing to amend claims 3, 13 and 21, but these amendments were not entered. Accordingly, the grounds of rejection that are on appeal are:

(1) The rejection of claims 1, 3, 11, 13, 19, and 21 as being obvious over Wood in view of Parker;

(2) The rejection of claims 2, 5, 12, 15, 20 and 23 as being obvious over Wood in view of Parker in view of Riggins;

(3) The rejection of claims 4, 6, 7, 10, 14, 16, 17, 22, 24 and 25 as being obvious over Wood in view of Parker in view of Olden; and

(4) The rejection of claims 8, 18 and 26 as being obvious over Wood in view of Parker in view of Butt.

For purposes of organizing the issues in this appeal, the appeal issues are discussed in four groups: (A) the obviousness rejections of claims 1, 3, 11, 13, 19 and 21 over at Wood and Parker listed above as appeal issue 1; and (B) the obviousness rejections of claims 2, 5, 12, 15, 20 and 23 listed above as issue 2; (C) the obviousness rejections of claims 4, 6, 7, 10, 14, 16, 17, 22, 24 and 25 listed above as issue 3; and (D) the obviousness rejections of claims 8, 18 and 26 listed above as issue 4.

VII. ARGUMENTS

A. Claims 1, 3, 11, 13, 19 and 21 Are Not Obvious Over Wood and Parker

Applicant appeals the obviousness rejection of claims 1, 3, 11, 13, 19 and 21 because none of the cited art references, taken singly or in combination, discloses using a single sign-on

(SSO) agent to not only (1) authenticate a user in response to an initial authentication request by obtaining or retrieving an attribute certificate having authentication data for the user, but also to (2) authenticate the user for subsequent authentication requests made by the SSO agent by using authentication data contained within the attribute certificate, as variously recited in claims 1, 11 and 19. *See, e.g.*, claim 1 ("authenticating the user at the SSO agent for the initial authentication request; retrieving by the SSO agent an attribute certificate associated with the user; and authenticating the user for subsequent authentication requests via the SSO agent using authentication data within the attribute certificate.") (emphasis added).

> The central role played by the SSO agent is described in the Application as follows:
>
> [0091] It should be noted that, in the preferred embodiment, the client SSO manager requests and receives an attribute certificate from an attribute certificate authority because it is assumed that the client SSO manager adheres to all PKIX protocols. By obtaining and storing an independently issued attribute certificate, the attribute certificate can be verified as an authenticate certificate by a third-party application. Moreover, if the client SSO manager were to be modified or replaced at some point in time, the attribute certificate could be independently verified as authenticate and then could be used by another SSO application.
>
> * * *
>
> [0093] After obtaining or generating the attribute certificate, thereby completing the configuration phase, user 510 will, at some subsequent point in time, desire to interact with one or more legacy applications 502 on application server 504. Using an appropriate protocol with client SSO manager 510, application server 504 initiates a session for user 500 and requests the user's authentication information for one or more legacy applications. For simplicity of presentation, it can be assumed that the user is initially attempting to access only a single protected resource.
>
> [0094] Preferably before, but possibly after, initiating the session with the application server, the client SSO manager challenges the user to complete an authentication process. Assuming that the user successfully completes this initial sign-on process, the client SSO manager acts as the user's agent to perform any subsequent authentication processing on behalf of the user.
>
> [0095] Continuing with the example, client SSO manager 510 retrieves attribute certificate 530 containing encrypted authentication attributes 526. Client SSO manager 510 locates the appropriate "SvceAuthInfo" attribute within attribute certificate 530 using the "service" field that corresponds to the legacy application that the user is attempted to access. Client SSO manager 510 then extracts the associated "authinfo" data for the corresponding legacy application.

U.S. Patent Publication No. 2002/0144119 (emphasis added).

In rejecting claims 1, 3, 11, 13, 19 and 21 as being obvious over Wood in view of Parker, the Examiner asserts that Woods teaches using a certificate for authentication in a single sign-on

system (citing Wood Patent, col. 5, lines 50-65). Final Office Action, p. 3. The Examiner asserts further that Woods discloses authenticating the user for subsequent authentication via the certificate (citing Woods Patent, col. 6, lines 4-10). Final Office Action, p. 3. Finally, while the Examiner concedes that Woods does not teach an attribute certificate, the Examiner invokes Parker (Parker Patent, col. 1, lines 45-50) in an attempt to remedy this deficiency in Wood.

In response, Applicant submits that the centrality of the SSO agent to the initial and subsequent authentication requests is simply not addressed by either of the cited Wood or Parker references, nor by the Examiner's analysis thereof. Indeed, Applicants have carefully reviewed the Woods passage cited by the Examiner to show "authenticating the user for subsequent authentication via the certificate," and there is simply no way that the cited passage supports the Examiner's assertion, as seen from the quoted passage:

> If the entity requesting access has not yet been authenticated to the trust level required for the particular access to the particular enterprise application or information resource requested, authorization component 140 may indicate that the access request is to be redirected to login component 120 so that login credentials may be obtained and authenticated to a particular trust level.

Woods Patent, col. 6, lines 4-10. As a review of this passage shows, there is no teaching or suggestion whatsoever that Wood's SSO retrieves an attribute certificate after performing an initial authentication, much less that the SSO uses authentication data within the retrieved attribute certificate to authenticate the user for subsequent authentication requests, as required by at least claims 1, 11, and 19. On this point, Applicant respectfully submits that the rejection analysis in no way acknowledges the specifically-claimed role of the SSO agent in both the initial authentication request and in the subsequent authentications requests. *See*, Final Office Action, p. 3. **Indeed, the cited passage from Wood confirms that, once login credentials are obtained for a user, "the access will typically be allowed without the need for further login credentials and authentication." Wood Patent, col. 6, lines 10-16. Thus, there are no "subsequent authentication requests" in the Wood scheme, much less "authenticating the user for subsequent authentication requests via the SSO agent using authentication data" as claimed.**

The foregoing deficiency is not remedied by Parker's disclosure of a system where the user (and not an SSO) is issued an attribute certificate. In addition, the cited passage from Parker offered by the Examiner to meet the requirement of an "attribute certificate" (Parker, col. 1, lines 40-50) confirms that the ***user*, and not any SSO agent, presents the privilege attribute**

certificate (PAC) to an application as evidence of the user's access rights. *See*, Parker, col. 1, lines 40-50 ("According to the invention there is provided a distributed computer system capable of supporting a plurality of users and a plurality of applications, the system including an authentication unit for authenticating a user and issuing that user with a privilege attribute certificate (PAC) which can then be presented to an application **by the user** as evidence of the user's access rights….") (emphasis added). Thus, Parker discloses that the *user* presents the privilege attribute certificate, and suggests no role for an SSO agent in this sequence.

Yet another defect in the rejection analysis of the final office action is that the motivational statement in the rejection fails to explain why one would have been motivated to employ the attribute certificates of Parker in the system of Wood. The motivational statement merely states that it would have been obvious "because the certificate is from a trusted secure source." Final Office Action, p. 4. Since every digital certificate is ostensibly created by a trusted secure source, the motivational statement merely recites a truism. More importantly, the rejection fails to explain the manner in which the teachings of the two references would be used within a hypothetical combination to form a new system with features from each reference. For example, it is unclear what entity in the system of Wood would obtain, manage, or use the attribute certificates of Parker and/or for what purpose. Thus, one cannot determine whether the incorporation of the usage of attribute certificates as taught by Parker into the system of Wood would benefit the implementation of a hypothetical system based on the system of Wood or whether it would be hinder the intended purpose of the system of Wood.

In the Advisory Action comments, the Examiner responds to the dual functional requirements of the SSO agent by asserting that:

> Woods (sic) teaches a single sign on system as shown in Columns 5, and 6 of US 6,691232. Woods teaches an SSO agent made of a login component, gatekeeper component, and other security components. Woods teache (sic, teaches) the user requests authentication from the SSO agent. The SSO agent retrieves from the user a credential such as a certificate, from the request. The SSO agent authenticates the suer (sic, user) for subsequent authentication request by establishing a Trust level, gained from the retrieved certificate.

Advisory Action, (Continuation Sheet). With all due respect, the broad and unspecified citation to two columns of text from the Woods Patent as disclosing "login component, gatekeeper component, and other security components" is entirely too vague and ambiguous for Applicant to understand how Woods allegedly meets the requirement of the claims. For example, the cited passages (including the reference to "login component, gatekeeper component, and other security

components," whatever they are) do not meet the specifically-claimed role of the SSO agent in both the initial authentication request and in the subsequent authentications requests. In particular, the selective citation of columns 5 and 6 does not disclose how Woods' "login component, gatekeeper component, and other security components" are used for "authenticating the user for subsequent authentication requests via the SSO agent using authentication data within the attribute certificate" as recited in the claims. Moreover, the Examiner's citation ignores the disclosure in Parker that the *user*, and not any SSO agent, presents the privilege attribute certificate (PAC) to an application as evidence of the user's access rights. *See*, Parker, col. 1, lines 40-50.

For at least the foregoing reasons, Applicant respectfully requests that the rejection be withdrawn because the Examiner has not made the *prima facie* obviousness showing that all the claim limitations are taught or suggested by the prior art. In re Royka, 490 F.2d 981, 180 USPQ 580 (CCPA 1974); In re Wilson, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970). Where a rejection is based on the assertion that all claim limitations are found in a number of prior art references, the fact finder must determine "[w]hat the prior art teaches, whether it teaches away from the claimed invention, and whether it motivates a combination of teachings from different references." In re Fulton, 391 F.3d 1195, 1199-1200 (Fed. Cir. 2004). The motivation-suggestion-teaching requirement "prevent[s] statutorily proscribed hindsight reasoning when determining the obviousness of an invention." Alza Corp. v. Mylan Labs., Inc., No. 06-1019 (Fed. Cir. Sept. 6, 2006). Thus, obviousness can only be established by combining the teachings of the Wood and Parker references to produce the claimed invention where there is some teaching, suggestion, or motivation to do so. In re Kahn, 441 F.3d 977, 986, 78 USPQ2d 1329, 1335 (Fed. Cir.2006) (discussing rationale underlying the motivation-suggestion-teaching requirement as a guard against using hindsight in an obviousness analysis.). As explained above, the proposed combination of Wood's SSO system for performing a single authentication with Parker's attribute certificate conflicts with Wood's disclosure that "the access will typically be allowed without the need for further login credentials and authentication." Wood Patent, col. 6, lines 10-16. In effect, Wood's disclosure that no further authentication will be required actually *teaches away* from Applicant's claim requirement of performing subsequent authentication requests by having the SSO retrieve an attribute certificate after performing an initial authentication, and then use authentication data within the retrieved attribute certificate to authenticate the user for subsequent authentication requests. When, as here, the Wood reference

teaches away from the proposed combination, a *prima facie* case of obviousness has been rebutted. *See*, MPEP § 2144.05(III) ("A *prima facie* case of obviousness may also be rebutted by showing that the art, in any material respect, teaches away from the claimed invention. In re Geisler, 116 F.3d 1465, 1471, 43 USPQ2d 1362, 1366 (Fed. Cir. 1997)…."). Applicants further submit that the Examiner's proposed combination of references is not sufficient to render the claims *prima facie* obvious because the proposed combination would change the principle of operation of the prior art invention being modified. In particular, the Wood reference discloses using an SSO to perform a single authentication for a given information resource, whereas the Parker reference discloses issuing a privilege attribute certificate to a user without any role being provided for an SSO. As a result, the proposed combination of Wood's SSO-based authentication approach with Parker would not be made by one of ordinary skill in the art since such a combination would change Parker's principle of operation whereby the user (and not an SSO) is issued a privilege attribute certificate. *See*, MPEP, § 2143.01(VI), *citing* In re Ratti, 270 F.2d 810, 123 USPQ 349 (CCPA 1959).

For at least the foregoing reasons, Applicant respectfully submits that a *prima facie* case of obviousness has not been established because neither Wood nor Parker disclose or suggest using an SSO agent to both (1) authenticate a user in response to an initial authentication request, and to (2) authenticate the user for subsequent authentication requests using authentication data from an attribute certificate that is retrieved the SSO agent. Accordingly, claims 1, 11 and 19 are allowable. To the extent that dependent claims 3, 13 and 21 each respectively incorporate the requirements of independent claims 1, 11 and 19, these dependent claims are likewise allowable, even though there are additional differences recited in the dependent claims. Accordingly, Applicant respectfully requests that the obviousness rejections of claims 1, 3, 11, 13, 19 and 21 over Wood and Parker be withdrawn and that the claims be allowed.

B. Claims 2, 5, 12, 15, 20 and 23 Are Not Obvious over Wood in View of Parker in view of Riggins

In response to the Examiner's rejection of claims 2, 5, 12, 15, 20 and 23 as being obvious over Wood, Parker and Riggins, Applicant respectfully requests reconsideration and withdrawal of the rejection because, as explained above with reference to independent claims 1, 11 and 19, none of the references disclose or suggest using a single sign-on (SSO) agent to not only (1) authenticate a user in response to an initial authentication request by obtaining or retrieving an attribute certificate having authentication data for the user, but also to (2) authenticate the user

for subsequent authentication requests made by the SSO agent by using authentication data contained within the attribute certificate, as variously recited in claims 1, 11 and 19. In particular, the deficiencies noted above with respect to Wood and Parker are not remedied by the disclosure of Riggins. While the final rejection relies on Riggins merely for its teaching of asymmetrical encryption, Applicant notes that Riggins fails to disclose an SSO that retrieves an attribute certificate after performing an initial authentication, and then uses authentication data within the retrieved attribute certificate to authenticate the user for subsequent authentication requests, as claimed. Thus, Riggins fails to remedy the deficiencies of a hypothetical combination of Woods and Parker.

In addition, the Examiner's proposed combination of Wood, Parker and Riggins to meet the claim requirements of performing multiple authentications conflicts with Wood's disclosure of an SSO that performs a single authentication for a given information resource. In effect, Woods disclosure actually *teaches away* from the claim requirements of performing multiple authentications. When, as here, the Wood reference teaches away from the proposed combination, a *prima facie* case of obviousness has been rebutted. *See*, MPEP § 2144.05(III) ("A *prima facie* case of obviousness may also be rebutted by showing that the art, in any material respect, teaches away from the claimed invention. In re Geisler, 116 F.3d 1465, 1471, 43 USPQ2d 1362, 1366 (Fed. Cir. 1997)…."). Applicants further submit that the Examiner's proposed combination of references is not sufficient to render the claims *prima facie* obvious because the proposed combination would change the principle of operation of the prior art invention being modified. In particular, the Wood reference discloses using an SSO to perform a single authentication for a given information resource, whereas the Parker reference discloses issuing a privilege attribute certificate to a user without any role being provided for an SSO. As a result, the proposed combination of Wood's SSO-based authentication approach with Parker would not be made by one of ordinary skill in the art since such a combination would change Parker's principle of operation whereby the user (and not an SSO) is issued a privilege attribute certificate. *See*, MPEP, § 2143.01(VI), *citing* In re Ratti, 270 F.2d 810, 123 USPQ 349 (CCPA 1959).

Applicant respectfully submits that it would not have been obvious for one having ordinary skill in the art to have used the applied prior art references to reach the claimed invention. Hence, a rejection of the claims cannot be based upon the cited prior art to establish a *prima facie* case of obviousness. Therefore, a rejection of the claims under 35 U.S.C. § 103(a)

has been shown to be insupportable in view of the cited prior art, and the claims are patentable over the applied references. Applicant respectfully requests the withdrawal of the rejection of the claims.

C. Claims 4, 6, 7, 10, 14, 16, 17, 22, 24 and 25 Are Not Obvious over Wood in View of Parker in view of Olden

In response to the Examiner's rejection of claims 4, 6, 7, 10, 14, 16, 17, 22, 24 and 25 as being obvious over Wood, Parker and Olden, Applicant respectfully requests reconsideration and withdrawal of the rejection because, as explained above with reference to independent claims 1, 11 and 19, none of the references disclose or suggest using a single sign-on (SSO) agent to not only (1) authenticate a user in response to an initial authentication request by obtaining or retrieving an attribute certificate having authentication data for the user, but also to (2) authenticate the user for subsequent authentication requests made by the SSO agent by using authentication data contained within the attribute certificate, as variously recited in claims 1, 11 and 19. In particular, the deficiencies noted above with respect to Wood and Parker are not remedied by the disclosure of Olden. While the final rejection relies on Olden merely for its teaching of interfacing with legacy applications, Applicant notes that Olden fails to disclose an SSO that retrieves an attribute certificate after performing an initial authentication, and then uses authentication data within the retrieved attribute certificate to authenticate the user for subsequent authentication requests, as claimed. Thus, Olden fails to remedy the deficiencies of a hypothetical combination of Woods and Parker.

In addition, the Examiner's proposed combination of Wood, Parker and Odento meet the claim requirements of performing multiple authentications conflicts with Wood's disclosure of an SSO that performs a single authentication for a given information resource. In effect, Woods disclosure actually *teaches away* from the claim requirements of performing multiple authentications. When, as here, the Wood reference teaches away from the proposed combination, a *prima facie* case of obviousness has been rebutted. *See*, MPEP § 2144.05(III) ("A *prima facie* case of obviousness may also be rebutted by showing that the art, in any material respect, teaches away from the claimed invention. In re Geisler, 116 F.3d 1465, 1471, 43 USPQ2d 1362, 1366 (Fed. Cir. 1997)…."). Applicants further submit that the Examiner's proposed combination of references is not sufficient to render the claims *prima facie* obvious because the proposed combination would change the principle of operation of the prior art invention being modified. In particular, the Wood reference discloses using an SSO to perform a

single authentication for a given information resource, whereas the Parker reference discloses issuing a privilege attribute certificate to a user without any role being provided for an SSO. As a result, the proposed combination of Wood's SSO-based authentication approach with Parker would not be made by one of ordinary skill in the art since such a combination would change Parker's principle of operation whereby the user (and not an SSO) is issued a privilege attribute certificate. *See*, MPEP, § 2143.01(VI), *citing* In re Ratti, 270 F.2d 810, 123 USPQ 349 (CCPA 1959).

Applicant respectfully submits that it would not have been obvious for one having ordinary skill in the art to have used the applied prior art references to reach the claimed invention. Hence, a rejection of the claims cannot be based upon the cited prior art to establish a *prima facie* case of obviousness. Therefore, a rejection of the claims under 35 U.S.C. § 103(a) has been shown to be insupportable in view of the cited prior art, and the claims are patentable over the applied references. Applicant respectfully requests the withdrawal of the rejection of the claims.

D. Claims 8, 18 and 26 Are Not Obvious over Wood in View of Parker in view of Butt

In response to the Examiner's rejection of claims 8, 18 and 26 as being obvious over Wood, Parker Butt, Applicant respectfully requests reconsideration and withdrawal of the rejections because, as explained above with reference to independent claims 1, 11 and 19, none of the references disclose or suggest using a single sign-on (SSO) agent to not only (1) authenticate a user in response to an initial authentication request by obtaining or retrieving an attribute certificate having authentication data for the user, but also to (2) authenticate the user for subsequent authentication requests made by the SSO agent by using authentication data contained within the attribute certificate, as variously recited in claims 1, 11 and 19. In particular, the deficiencies noted above with respect to Wood and Parker are not remedied by the disclosure of Butt. While the final rejection relies on Butt merely for its teaching of X.509 digital certificates, Applicant notes that Butt fails to disclose an SSO that retrieves an attribute certificate after performing an initial authentication, and then uses authentication data within the retrieved attribute certificate to authenticate the user for subsequent authentication requests, as claimed. Thus, Butt fails to remedy the deficiencies of a hypothetical combination of Woods and Parker.

In addition, the Examiner's proposed combination of Wood, Parker and Butt to meet the claim requirements of performing multiple authentications conflicts with Wood's disclosure of an SSO that performs a single authentication for a given information resource. In effect, Woods disclosure actually *teaches away* from the claim requirements of performing multiple authentications. When, as here, the Wood reference teaches away from the proposed combination, a *prima facie* case of obviousness has been rebutted. *See*, MPEP § 2144.05(III) ("A *prima facie* case of obviousness may also be rebutted by showing that the art, in any material respect, teaches away from the claimed invention. In re Geisler, 116 F.3d 1465, 1471, 43 USPQ2d 1362, 1366 (Fed. Cir. 1997)…."). Applicants further submit that the Examiner's proposed combination of references is not sufficient to render the claims *prima facie* obvious because the proposed combination would change the principle of operation of the prior art invention being modified. In particular, the Wood reference discloses using an SSO to perform a single authentication for a given information resource, whereas the Parker reference discloses issuing a privilege attribute certificate to a user without any role being provided for an SSO. As a result, the proposed combination of Wood's SSO-based authentication approach with Parker would not be made by one of ordinary skill in the art since such a combination would change Parker's principle of operation whereby the user (and not an SSO) is issued a privilege attribute certificate. *See*, MPEP, § 2143.01(VI), *citing* In re Ratti, 270 F.2d 810, 123 USPQ 349 (CCPA 1959).

Applicant respectfully submits that it would not have been obvious for one having ordinary skill in the art to have used the applied prior art references to reach the claimed invention. Hence, a rejection of the claims cannot be based upon the cited prior art to establish a *prima facie* case of obviousness. Therefore, a rejection of the claims under 35 U.S.C. § 103(a) has been shown to be insupportable in view of the cited prior art, and the claims are patentable over the applied references. Applicant respectfully requests the withdrawal of the rejection of the claims.

VIII. CLAIMS APPENDIX - 37 CFR § 41.37(c)(1)(viii)

A copy of the pending claims involved in the appeal is attached as Appendix "B."

IX. EVIDENCE APPENDIX - 37 CFR § 41.37(c)(1)(ix)

None.

X. RELATED PROCEEDINGS APPENDIX - 37 CFR § 41.37(c)(1)(x)

There are no related proceedings.

XI. CONCLUSION

A *prima facie* case of obviousness has not been established because none of the cited references discloses Applicant's use of an SSO agent for authenticating a user for an initial and subsequent authentication requests using authentication data from an attribute certificate obtained by the SSO agent. In view of the above arguments, it is respectfully urged that the rejection of the claims should not be sustained.

FILED ELECTRONICALLY
December 7, 2007

Respectfully submitted,

/Michael Rocco Cannatti/

Michael Rocco Cannatti
Attorney for Applicant
Reg. No. 34,791

APPENDIX A - RELATED APPEALS AND INTERFERENCES

There are no decisions rendered by a court or the Board in any related proceeding.

APPENDIX B - PENDING CLAIMS

1. (Original) A method for an authentication process within a data processing system, the method comprising:

receiving at a single sign-on (SSO) agent an initial authentication request for a user;

authenticating the user at the SSO agent for the initial authentication request;

retrieving by the SSO agent an attribute certificate associated with the user; and

authenticating the user for subsequent authentication requests via the SSO agent using authentication data within the attribute certificate.

2. (Original) The method of claim 1 further comprising:

retrieving a private key associated with the user;

extracting encrypted authentication data from the attribute certificate, wherein the encrypted authentication data was generated by encrypting authentication data with a public key associated with the user; and

decrypting the encrypted authentication data locally using the private key associated with the user in order to extract authentication data for a protected resource.

3. (Original) The method of claim 1 further comprising:

forwarding the authentication data to a protected resource.

4. (Original) The method of claim 3 wherein the protected resource is a legacy application.

5. (Original) The method of claim 3 further comprising:

approving the user for access to the protected resource based on the authentication data.

6. (Original) The method of claim 3, wherein the attribute certificate contains multiple sets of authentication data for multiple protected resources, the method further comprising:

parsing the authentication data to retrieve a specific set of authentication data for the protected resource.

7. (Original) The method of claim 1 wherein the authentication data comprises a user identity and a password.

8. (Original) The method of claim 1 wherein the attribute certificate is formatted according to an X.509 standard.

9. (Original) A data structure representing an attribute certificate for use in a data processing system, the data structure comprising:

an issuer name;

a signature;

a holder name;

an attribute containing encrypted authentication data that was generated by encrypting multiple sets of authentication data for protected resources with a public key associated with a user by a network single sign-on (SSO) agent.

10. (Original) The data structure of claim 9 wherein the protected resource is a legacy application.

11. (Original) An apparatus for an authentication process within a data processing system, the apparatus comprising:

means for receiving at a single sign-on (SSO) agent an initial authentication request for a user;

means for authenticating the user at the SSO agent for the initial authentication request;

means for retrieving by the SSO agent an attribute certificate associated with the user; and

means for authenticating the user for subsequent authentication requests via the SSO agent using authentication data within the attribute certificate.

12. (Original) The apparatus of claim 11 further comprising:

means for retrieving a private key associated with the user;

means for extracting encrypted authentication data from the attribute certificate, wherein the encrypted authentication data was generated by encrypting authentication data with a public key associated with the user; and

means for decrypting the encrypted authentication data locally using the private key associated with the user in order to extract authentication data for a protected resource.

13. (Original) The apparatus of claim 11 further comprising:

means for forwarding the authentication data from the SSO agent to a protected resource.

14. (Original) The apparatus of claim 13 wherein the protected resource is a legacy application.

15. (Original) The apparatus of claim 13 further comprising:

means for approving the user for access to the protected resource based on the authentication data.

16. (Original) The apparatus of claim 13, wherein the attribute certificate contains multiple sets of authentication data for multiple protected resources, the apparatus further comprising:

means for parsing the authentication data to retrieve a specific set of authentication data for the protected resource.

17. (Original) The apparatus of claim 11 wherein the authentication data comprises a user identity and a password.

18. (Original) The apparatus of claim 11 wherein the attribute certificate is formatted according to an X.509 standard.

19. (Original) A computer program product in a computer-readable medium for use in a data processing system for an authentication process, the computer program product comprising:

instructions for receiving at a single sign-on (SSO) agent an initial authentication request for a user;

instructions for authenticating the user at the SSO agent for the initial authentication request;

instructions for retrieving by the SSO agent an attribute certificate associated with the user; and

instructions for authenticating the user for subsequent authentication requests via the SSO agent using authentication data within the attribute certificate.

20. (Original) The computer program product of claim 19 further comprising:

instructions for retrieving a private key associated with the user;

instructions for extracting encrypted authentication data from the attribute certificate, wherein the encrypted authentication data was generated by encrypting authentication data with a public key associated with the user; and

instructions for decrypting the encrypted authentication data locally using the private key associated with the user in order to extract authentication data for a protected resource.

21. (Original) The computer program product of claim 19 further comprising: instructions for forwarding the authentication data from the SSO agent to a protected resource.

22. (Original) The computer program product of claim 21 wherein the protected resource is a legacy application.

23. (Original) The computer program product of claim 21 further comprising:
instructions for approving the user for access to the protected resource based on the authentication data.

24. (Original) The computer program product of claim 21, wherein the attribute certificate contains multiple sets of authentication data for multiple protected resources, the computer program product further comprising:
instructions for parsing the authentication data to retrieve a specific set of authentication data for the protected resource.

25. (Original) The computer program product of claim 19 wherein the authentication data comprises a user identity and a password.

26. (Original) The computer program product of claim 19 wherein the attribute certificate is formatted according to an X.509 standard.

APPENDIX C

1. A method for an authentication process within a data processing system, the method comprising:

receiving at a single sign-on (SSO) agent (510) an initial authentication request for a user (500);

authenticating the user at the SSO agent (510) for the initial authentication request;

retrieving by the SSO agent an attribute certificate (530) associated with the user (500); and

authenticating the user (500) for subsequent authentication requests via the SSO agent (510) using authentication data (526) within the attribute certificate (530).

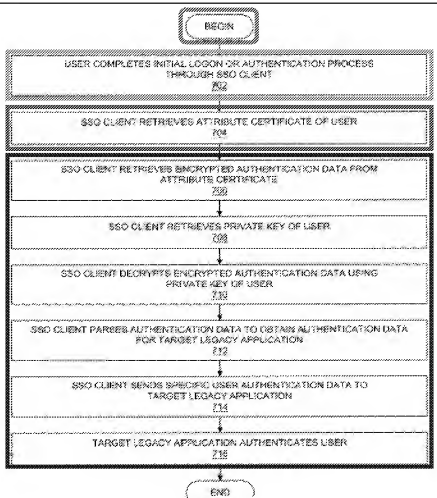

FIG. 7

9. A data structure representing an attribute certificate for use in a data processing system, the data structure comprising:

an issuer name;

a signature;

a holder name;

an attribute containing encrypted authentication data that was generated by encrypting multiple sets of authentication data for protected resources with a public key associated with a user by a network single sign-on (SSO) agent.

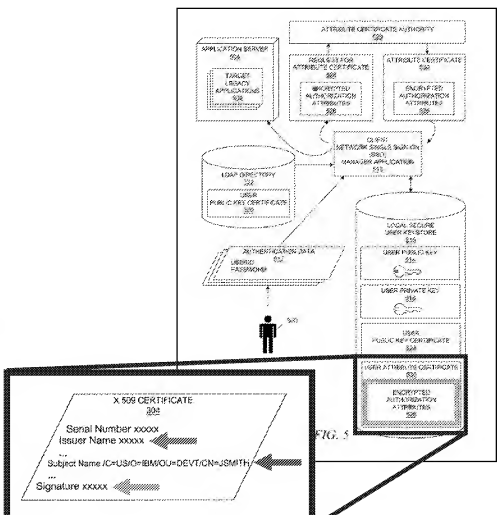

FIG. 5

11. An apparatus for an authentication process within a data processing system, the apparatus comprising:

means for receiving at a single sign-on (SSO) agent an initial authentication request for a user;

means for authenticating the user at the SSO agent for the initial authentication request;

means for retrieving by the SSO agent an attribute certificate associated with the user; and

means for authenticating the user for subsequent authentication requests via the SSO agent using authentication data within the attribute certificate.

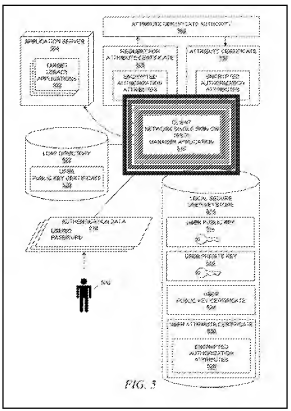

FIG. 5

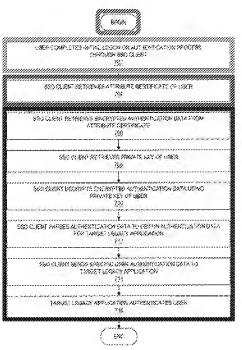

FIG. 7

19. A computer program product in a computer-readable medium for use in a data processing system for an authentication process, the computer program product comprising:

instructions for receiving at a single sign-on (SSO) agent an initial authentication request for a user;

instructions for authenticating the user at the SSO agent for the initial authentication request;

instructions for retrieving by the SSO agent an attribute certificate associated with the user; and

instructions for authenticating the user for subsequent authentication requests via the SSO agent using authentication data within the attribute certificate.

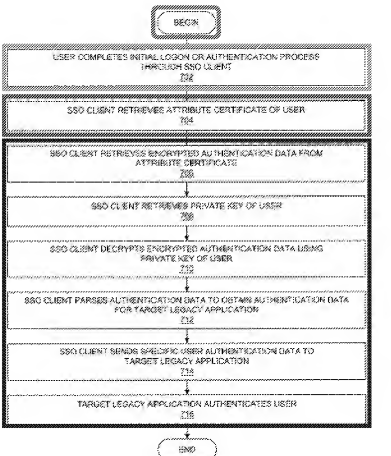

FIG. 7